In the Claims

A complete listing of all claims follows. Please amend claims 1 – 4 and add the following new claims 5 – 95:

1. (Currently amended) A method for selectively allowing or denying access to a user coupled to an electronic communications network, said user having an associated recipient identifier, comprising the steps of:

A. generating a plurality of proxy identifiers associated with said user, each of said proxy identifiers having at least three associated security states, a first of said states being indicative of allowing any party coupled to said network access to said user, a second of said states being indicative of denying any party coupled to said network access to said user, and a third of said states being conditionally indicative of allowing at least one but fewer than all parties coupled to said network access to said user if predetermined criteria are met and denying access to said user otherwise;

B. in response to an inbound message from said network including ~~said~~ a sender identifier and ~~a~~ said recipient identifier, said sender identifier being associated with ~~the~~ a sender of said inbound message, transfer said inbound message to a location associated with one of said proxy identifiers;

C. processing said transferred inbound message to evaluate a security status associated therewith, said security status being related to said sender identifier and said recipient identifier~~,~~ ; and

D. allowing access for said transferred message to said user when said security status meets one or more predetermined criteria at least partially related to said security status of said one proxy identifier, and denying access for said transferred message to said user otherwise.

2. (Currently amended) The method of claim 1, wherein said identifiers are e-mail addresses.

3. (Currently amended) A system for selectively allowing or denying access to a user coupled to an electronic communications network, said user having an associated recipient identifier, comprising ~~the steps of~~:

A. a generator for generating a plurality of proxy identifiers associated with said user, each of said proxy identifiers having at least three associated security states, a first of said states being indicative of allowing any party coupled to said network access to said user, a second of said states being indicative of denying any party coupled to said network access to said user, and a third of said states being conditionally indicative of allowing at least one but fewer than all parties coupled to said network access to said user if predetermined criteria are met and denying access to said user otherwise;

B. a message transferor responsive to an inbound message from said network including ~~said~~ a sender identifier and ~~a~~ said recipient identifier, said sender identifier being associated with ~~the~~ a sender of said inbound message, to transfer said inbound message to a location associated with one of said proxy identifiers;

C. a processor for evaluating a security status associated with said transferred inbound message, said security status being related to said sender identifier and said recipient identifier, and

D. a gate for allowing access for said transferred message to said user when said security status meets one or more predetermined criteria at least partially related to said security states of said one proxy identifier, and denying access for said transferred message to said user otherwise.

4. (Currently amended) The system of claim 3, wherein said identifiers are e-mail addresses.

5. (New) The method of claim 1, wherein at least one of the generated proxy identifiers associated with said user is substantially absent content that identifies said user.

6. (New) The method of claim 1, wherein at least one of the generated proxy identifiers associated with said user is valid for a predefined time period.

7. (New) The method of claim 1, wherein the plurality of proxy identifiers are stored in a database.

8. (New) The method of claim 7, wherein an entry in the database includes data representing a contact name associated with said user, a proxy address assigned to said user, and the security state associated with the proxy address.

9. (New) The method of claim 1, wherein processing said transferred inbound message includes attempting to match said recipient identifier with at least one of the plurality of proxy identifiers associated with said user.

10. (New) The method of claim 1, wherein processing said transferred inbound message includes attempting to match said sender identifier with at least one of a plurality of identifiers associated with contacts of the user.

11. (New) The method of claim 1, wherein processing said transferred inbound message includes determining the security state associated with said user.

12. (New) The method of claim 1, wherein denying transfer of said message to said user includes sending a reply message to said sender.

13. (New) The method of claim 1, wherein denying transfer of said message to said user includes sending a reply message to said sender, wherein said reply message includes one of said plurality of proxy identifiers associated with said user.

14. (New) The method of claim 1, wherein denying transfer of said message to said user includes generating a proxy identifier associated with said user and sending a reply message to said sender, wherein said reply message includes the generated proxy identifier associated with said user.

15. (New) The method of claim 1, wherein denying transfer of said message to said user includes entering said sender identifier into a database.

16. (New) The method of claim 1, wherein allowing transfer of said message to said user includes determining if said user replied to a message previously sent from said sender.

17. (New) The method of claim 1, wherein allowing transfer of said message to said user includes determining if said user initiated generation of a proxy identifier included in the message.

18. (New) The method of claim 17, wherein said user-generated proxy identifier is absent from said plurality of proxy identifiers.

19. (New) The method of claim 18, further comprising the step:

if said user-generated proxy identifier is absent from said plurality of proxy identifiers, adding said user generated proxy identifier to said plurality of proxy identifiers.

20. (New) The method of claim 17, wherein allowing transfer of said message to said user includes removing reference to said user-generated proxy identifier in said message.

21. (New) The method of claim 17, wherein allowing transfer of said message to said user includes removing reference to said user-generated proxy identifier in said message and adding an e-mail address associated with said user to said message.

22. (New) The method of claim 1, wherein processing said inbound message includes removing reference to said recipient identifier included in said message.

23. (New) The method of claim 1, wherein said first state that is indicative of allowing any party coupled to said network access to said user, includes allowing transfer of a message from said party to said user.

24. (New) The method of claim 1, wherein said second state that is indicative of denying any party coupled to said network access to said user, includes blocking transfer of a message from said any party to said user.

25. (New) The method of claim 1, wherein said predetermined criteria includes the user previously responding to a message previously sent by the sender.

26. (New) The method of claim 25, wherein said previously sent message includes said sender identifier.

27. (New) The method of claim 1, wherein one of the predetermined criteria includes the sender identifier matching one of a plurality of identifiers.

29. (New) The method of claim 1, wherein one of the predetermined criteria includes the recipient identifier matching one of the plurality of proxy identifiers.

30. (New) The method of claim 1, wherein one of the predetermined criteria includes both the recipient identifier and the sender identifier are associated with the same network domain.

31. (New) A method for selectively allowing or denying access to a user coupled to an electronic communications network, comprising the steps of:

receiving an inbound message over the electronic communications network from a sender, wherein the inbound message includes an identifier associated with a sender and an identifier associated with a recipient; and

determining one of at least three security states associated with the inbound message, wherein a first security state is indicative of allowing delivery of the inbound message to the user, a second security state is indicative of denying delivery of the inbound message to the user, a third security state is indicative of conditionally allowing delivery of the message to the user, each of the at least three security states are associated with the sender identifier and the recipient identifier included in the inbound message.

32. (New) The method of claim 31, wherein determining one of the at least three security states includes determining if the recipient identifier matches one of a plurality of proxy identifiers.

33. (New) The method of claim 31, further comprising:

prior to delivery, replacing each reference to the recipient identifier in the message with an identifier associated with the user if the recipient identifier matches one of a plurality of proxy identifiers.

34. (New) The method of claim 31, wherein determining one of the at least three security states includes determining if the sender identifier matches one of a plurality of sender identifiers.

35. (New) The method of claim 31, wherein the recipient identifier is a proxy identifier that is substantially absent content that identifies said user.

36. (New) The method of claim 31, wherein the identifiers are e-mail addresses.

37. (New) The method of claim 31, wherein detecting the second security state initiates sending a reply message to the sender to report the delivery denial.

38. (New) The method of claim 31, wherein detecting the second security state initiates sending a reply message to the sender that reports the delivery denial, wherein the reply message includes a proxy identifier associated with the user for sending a future message.

39. (New) The method of claim 31, wherein detecting the third security state associates an alert indicator with the message.

40. (New) The method of claim 39, wherein the alert indicator includes a flag that is associated with the message.

41. (New) The method of claim 31, wherein the third security state is triggered if the message is a response to a message previously sent by the user to the sender.

42. (New) The method of claim 31, wherein the third security state is triggered if the recipient identifier included in the message is a proxy identifier generated by the user and is absent from the plurality of proxy identifiers.

43. (New) The method of claim 31, wherein the third security state is triggered if the recipient identifier and the sender identifier include the same network domain.

44. (New) The method of claim 31, wherein the recipient identifier is a proxy identifier assigned to the user for a period of time.

45. (New) The system of claim 3, wherein at least one of the generated proxy identifiers associated with said user is substantially absent content that identifies said user.

46. (New) The system of claim 3, wherein at least one of the generated proxy identifiers associated with said user is valid for a predefined time period.

47. (New) The system of claim 3, further comprising:

a database configured to store the plurality of proxy identifiers.

48. (New) The system of claim 47, wherein the database includes an entry that stores data that represents a contact name associated with said user, a proxy identifier assigned to said user, and the security state associated with the proxy address.

49. (New) The system of claim 3, wherein the processor attempts to match said sender identifier with a least one of a plurality of identifiers associated with the user.

50. (New) The system of claim 3, wherein the processor determines the security state associated with said user that overrides the security state associated with the message.

51. (New) The system of claim 3, wherein the processor determines if said recipient identifier matches one of said plurality of proxy identifiers associated with said user.

52. (New) The system of claim 3, wherein the gate initiates sending a reply message to said sender to report denying transfer of said message.

53. (New) The system of claim 3, wherein the gate initiates sending a reply message to said sender to report denying transfer of said message, wherein said reply message includes one of said plurality of proxy identifiers associated with said user.

54. (New) The system of claim 3, wherein the processor initiates entering said sender identifier into a database when access to the user by transferring said message is denied.

55. (New) The system of claim 3, wherein the processor determines if said user replied to a previously sent message from said sender to determine whether to transfer said message to said user.

56. (New) The system of claim 3, wherein the processor determines if said user initiated generation of said recipient identifier to determine whether to transfer said message to said user.

57. (New) The system of claim 56, wherein said user-generated recipient identifier is absent from said plurality of proxy identifiers.

58. (New) The system of claim 57, wherein if said processor determines that said user-generated recipient identifier is absent, said processor initiates adding said user-generated recipient identifier into said plurality of proxy identifiers.

59. (New) The system of claim 3, wherein if said message is transferred to said user, said processor initiates removing from any reference to said recipient identifier from said message.

60. (New) The system of claim 3, wherein if said message is transferred to said user, said processor initiates adding a reference to an identifier associated with the recipient in said message.

61. (New) The system of claim 3, wherein if said first security state is detected, the gate allows transfer of said inbound to said user.

62. (New) The system of claim 3, wherein if said second state is detected, the gate blocks transfer of said inbound message to said user.

63. (New) The system of claim 3, wherein said predetermined criteria includes the user responding to a previously sent message from said sender.

64. (New) The system of claim 63, wherein said previously sent message includes the sender identifier.

65. (New) The system of claim 3, wherein the predetermined criteria includes the processor matching the sender identifier to one of a plurality of identifiers.

66. (New) The system of claim 3, wherein the predetermined criteria includes the processor matching the recipient identifier to one of the plurality of proxy identifiers.

67. (New) The system of claim 3, wherein the predetermined criteria includes the processor determining that the recipient identifier and the sender identifier are associated with the same network domain.

68. (New) A system for selectively allowing or denying access to a user coupled to an electronic communications network, comprising:

a receiver configured to receive an inbound message over the electronic communications network from a sender, wherein the inbound message includes an identifier of the sender and an identifier of the recipient; and

a processor configured to determine one of at least three security states associated with the inbound message, wherein a first security state is indicative of allowing delivery of the inbound message to the user, a second security state is indicative of denying delivery of the inbound message to the user, a third security state is indicative of conditionally allowing delivery of the message to the user, each of the at least three security states are associated with the sender identifier and the recipient identifier included in the inbound message.

69. (New) The system of claim 68, wherein the processor determines if the recipient identifier matches one of a plurality of proxy identifiers to determine one of the at least three security states.

70. (New) The system of claim 68, wherein prior to delivery, the processor is configured to replace each reference to the recipient identifier in the message with an identifier of the user if the recipient identifier matches one of a plurality of proxy identifiers.

71. (New) The system of claim 68, wherein the processor is configured to determine if the sender identifier matches one of a plurality of sender identifiers.

72. (New) The system of claim 68, wherein the recipient identifier is a proxy identifier that is substantially absent content that identifies said user.

73. (New) The system of claim 68, wherein the identifiers are e-mail addresses.

74. (New) The system of claim 68, wherein when the second security state is detected, the processor initiates sending a reply message to the sender to report the delivery denial.

75. (New) The system of claim 68, wherein when the second security state is detected, the processor initiates sending a reply message to the sender to report the delivery denial, wherein the reply message includes a proxy identifier to send a future message.

76. (New) The system of claim 68, wherein when the third security state is detected, an alert indicator is associated with the message.

77. (New) The system of claim 76, wherein the alert indicator includes a flag that is associated with the message.

78. (New) The system of claim 68, wherein the third security state is triggered if the message is a response to a previously sent message from the user to the sender.

79. (New) The system of claim 68, wherein the third security state is triggered if the recipient identifier is a proxy identifier generated by the user and is absent from a plurality of proxy identifiers associated with the user that are stored in a database.

80. (New) The system of claim 68, wherein the third security state is triggered if the user identifier and the sender identifier include the same network domain.

81. (New) The system of claim 68, wherein the recipient identifier is assigned to the user for a period of time.

82. (New) A computer program product residing on a computer readable medium having a plurality of instructions stored thereon which, when executed by a processor, cause that processor to:

receive an inbound message over a electronic communications network from a sender, wherein the inbound message includes an identifier of the sender and an identifier of a recipient; and

determine one of at least three security states associated with the inbound message, wherein a first security state is indicative of allowing delivery of the inbound message to a user, a second security state is indicative of denying delivery of the inbound message to the user, a third security state is indicative of conditionally allowing delivery of the message to the user, each of the at least three security states are associated with the sender identifier and the recipient identifier included in the inbound message.

83. (New) The computer program product of claim 82, wherein to determine one of the at least three security states includes determining if the recipient identifier matches one of a plurality of proxy identifiers.

84. (New) The computer program product of claim 82, further comprising instructions for:

prior to delivery, if the recipient identifier matches one of a plurality of proxy identifiers, replacing each reference of the recipient identifier in the message with an identifier associated with the user.

85. (New) The computer program product of claim 82, wherein to determine one of the at least three security states includes determining if the sender identifier matches one of a plurality of sender identifiers.

86. (New) The computer program product of claim 82, wherein the recipient identifier is a proxy identifier that is substantially absent content that identifies said user.

87. (New) The computer program product of claim 82, wherein the identifiers are e-mail addresses.

88. (New) The computer program product of claim 82, further comprising instructions for:

upon detecting the second security state, sending a reply message to the sender to report delivery denial.

89. (New) The computer program product of claim 82, further comprising instructions for:

upon detecting the second security state, sending a reply message to the sender that reports the delivery denial, wherein the reply message includes a proxy address to send a future message.

90. (New) The computer program product of claim 82, further comprising instructions for:

upon detecting the third security state, associating an alert indicator with the message.

91. (New) The computer program product of claim 90, wherein the alert indicator includes a flag that is associated with the message.

92. (New) The computer program product of claim 82, wherein the third security state is triggered if the message is a response to a previously sent message from the user to the sender.

93. (New) The computer program product of claim 82, wherein the third security state is triggered if the recipient identifier in the message is a proxy identifier generated by the

user and is absent from a plurality of proxy identifiers that are associated with the user and stored in a database.

94. (New) The computer program product of claim 82, wherein the third security state is triggered if the recipient identifier and the sender identifier include the same network domain.

95. (New) The computer program product of claim 82, wherein the recipient identifier is assigned to the user for a period of time.